UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/930,029	08/14/2001	William B. Sweet	055120-0002	3170

7590 04/05/2006

William Sweet
2665 North First St
Suite 300
San Jose, CA 95134

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/930,029	SWEET ET AL.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22 and 52-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22 and 52-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Remarks

Claims 1-22 and 52-58 are pending.

Response to Arguments

Applicant's arguments, see Remarks, filed 1/13/2006, with respect to the rejection(s) of claim(s) 1-22 and 52-58 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made with Win (U.S. Patent 6,161,139) in view of Berson (U.S. Patent 6,754,821), Woodward (Woodward, John, "Comments on Private Sector Use of Biometrics and the Need for Limited Government Action", 7/17/1998, pp. 1-12, obtained from http://www.ntia.doc.gov/ntiahome/privacy/mail/disk/Woodward.htm), and Shintani (U.S. Patent 6,137,480).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1, 15, 16, 18-22, 52, and 54-57 are rejected under 35 U.S.C. 102(e) as being anticipated by Win (U.S. Patent 6,161,139).

Regarding Claim 1,

Win discloses a method for providing cryptographic capabilities to a plurality of network users over a decentralized public network, comprising:

Receiving a request for an access permission security profile on behalf of a network user (Column 9, lines 25-45);

Authenticating the request (Column 9, lines 36-45; and Column 10, lines 26-40);

Creating the access permission security profile, to be used in forming a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object and to encrypt selected portions of a plaintext object (Column 10, lines 26-40); and

Securely transmitting the access permission security profile to the network user over the network (Column 10, lines 41-49).

Regarding Claim 15,

Win discloses the method of claim 1, in addition, Win discloses that the request is initiated in-band by the network user over the network (Column 9, lines 25-35).

Regarding Claim 16,

Win discloses the method of claim 1, in addition, Win discloses that the access permission security profile is in the form of a token that is adaptable to expire (Column 10, lines 50-62).

Regarding Claim 18,

Win discloses the method of claim 1, in addition, Win discloses that the authenticating step includes the use of a hardware token (Column 27, lines 28-40).

Regarding Claim 19,

Win discloses the method of claim 1, in addition, Win discloses that the authenticating step includes the use of a software token (Column 17, lines 24-33).

Regarding Claim 20,

Win discloses the method of claim 1, in addition, Win discloses that the authenticating step includes the use of a user password (Column 9, lines 25-35).

Regarding Claim 21,

Win discloses the method of claim 1, in addition, Win discloses that the authenticating step includes the use of a record of time at which the request was made (Column 9, lines 46-52).

Regarding Claim 22,

Win discloses the method of claim 1, in addition, Win discloses that the authenticating step includes the use of a record of the user's physical location (Column 15, lines 46-60).

Regarding Claim 52,

Win discloses a centralized security management system for distributing cryptographic capabilities to a plurality of network users over a decentralized public network, comprising:

A plurality of member tokens for providing cryptographic capabilities to authenticated users of the decentralized public network (Column 13, lines 32-44);

A set if server systems for managing the distribution of member tokens (Figure 1);

Means for requesting a member token from at least one server system (Column 9, lines 25-45);

A set of client systems (Column 4, lines 10-44), wherein each client system includes means for receiving the requested member token (Column 10, lines 26-49) and means for utilizing the cryptographic capabilities provided by the member token (Column 7, line 53 to Column 8, line 16); and

Means for securely distributing a requested member token from at least one server system to at least one client system over the decentralized public network (Column 10, lines 41-49).

Regarding Claim 54,

Win discloses that the means for requesting a member token resides on each client system (Column 9, lines 25-45).

Regarding Claim 55,

Win discloses that means for authenticating a user resides on at least one server system (Column 10, lines 26-40).

Regarding Claim 56,

Win discloses that managing the distribution of member tokens includes dynamic updating of the member tokens (Column 17, lines 37-48).

Regarding Claim 57,

Win discloses the method of claim 1 and the system of claim 52, in addition, Win discloses that the decentralized public network is the Internet (Column 4, lines 46-57).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 2-16, 18-22, 57, and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Win in view of Berson (U.S. Patent 6,754,821).

Regarding Claim 2,

Win discloses that the creating step comprises:

Identifying one or more groups of network users who are to be provided with cryptographic capabilities (Column 10, lines 26-49; and Column 13, lines 32-44); and

Creating one or more security profiles for each network user (Column 13, lines 32-44);

But does not disclose establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key, or that the security profiles contain at least one of these access codes.

Berson, however, discloses establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key (Column 3, lines 23-34; and Column 5, lines 20-35); and

That each network user's security profile contains at least one access code (Column 5, line 20 to Column 6, line 8).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the transition state-based cryptography system of Berson into the role-based access control system of Win in order to allow an entire file, program, etc. to be downloaded/acquired at first, while controlling access to

different/progressive sections of the data based upon predetermined conditions that the user must meet prior to decryption of the additional sections.

Regarding Claim 3,

Win as modified by Berson discloses the method of claim 2, in addition, Win discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup, or domain (Column 13, lines 32-44).

Regarding Claim 4,

Win discloses a method for providing decryption capabilities to a plurality of network users over a decentralized public network, comprising:

Receiving a request for decryption capabilities on behalf of a network user (Column 9, lines 25-45);

Authenticating the request (Column 9, lines 36-45; and Column 10, lines 26-40);

Creating an access permission security profile to be used in forming a cryptographic key for enabling the network user to decrypt an encrypted object (Column 10, lines 26-40);

Receiving from the user information associated with the encrypted object (Column 7, line 53 to Column 8, line 3); and

Session/transaction encryption (Column 22, lines 15-65);

But does not disclose generating a cryptographic key using the access permission security profile and the received information associated with the encrypted object, and securely transmitting the cryptographic key to the network user over the network.

Berson, however, discloses generating a cryptographic key using the access permission security profile and the received information associated with the encrypted object (Column 5, line 56 to Column 6, line 8); and securely transmitting the cryptographic key to the network user over the network (Column 5, line 36 to Column 6, line 8). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the transition state-based cryptography system of Berson into the role-based access control system of Win in order to allow an entire file, program, etc. to be downloaded/acquired at first, while controlling access to different/progressive sections of the data based upon predetermined conditions that the user must meet prior to decryption of the additional sections.

Regarding Claim 5,

Win as modified by Berson discloses the method of claim 4, in addition, Win discloses that the creating step comprises:

Identifying one or more groups of network users who are to be provided with cryptographic capabilities (Column 10, lines 26-49; and Column 13, lines 32-44); and

Creating one or more security profiles for each network user (Column 13, lines 32-44); and

Berson discloses establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key (Column 3, lines 23-34; and Column 5, lines 20-35); and

That each network user's security profile contains at least one access code (Column 5, line 20 to Column 6, line 8).

Regarding Claim 6,

Win as modified by Berson discloses the method of claim 5, in addition, Win discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup or domain (Column 13, lines 32-44).

Regarding Claim 7,

Win discloses a method for cryptographically securing the distribution of information over a decentralized public network to a plurality of network users, comprising:

Creating a computer representable data object (Column 14, line 25 to Column 15, line 14);

Creating one or more access permission credentials (Column 17, line 65 to Column 18, line 10);

Assigning an access permission credential to each of the data objects, wherein the access permission credential ensures that only authorized users are able to access the data objects (Column 17, line 65 to Column 18, line 57);

Authorizing at least one network user from the plurality of network users (Column 8, lines 17-44); and

Transmitting the data object over the network (Column 8, lines 45-60);

But does not disclose the encryption of embedded objects within each data object, or the access to/decryption of selected embedded objects.

Berson, however, discloses that a data object includes one or more embedded objects (Column 3, lines 23-34; and Column 5, lines 20-35);

Selecting one or more embedded objects of the data object to be encrypted (Column 3, lines 23-34; and Column 5, lines 20-35);

Encrypting the selected embedded objects (Column 3, lines 23-34; and Column 5, lines 20-35); and

Assigning an access permission credential to each of the selected embedded objects, wherein the access permission credential ensures that only authorized users are able to decrypt encrypted embedded objects of the data object (Column 5, line 20 to Column 6, line 8).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the transition state-based cryptography system of Berson into the role-based access control system of Win in order to allow an entire file, program, etc. to be downloaded/acquired at first, while controlling access to different/progressive sections of the data based upon predetermined conditions that the user must meet prior to decryption of the additional sections.

Regarding Claim 8,

Win as modified by Berson discloses the method of claim 7, in addition, Win discloses that the information is digital content (Column 9, lines 26-35).

Regarding Claim 9,

Win as modified by Berson discloses the method of claim 7, in addition, Win discloses that the authorizing step includes:

Receiving a request for an access permission security profile on behalf of a network user (Column 9, lines 25-45);

Authenticating the request (Column 9, lines 36-45; and Column 10, lines 26-40); and

Securely transmitting the security profile to the network user over the network (Column 10, lines 41-49).

Regarding Claim 10,

Win as modified by Berson discloses the method of claim 7, in addition, Win discloses that the authorizing step includes:

Sending a request for an access permission security profile on behalf of a network user to a centralized server system over the network (Column 9, lines 25-45);

Receiving the request at the central server system (Column 9, lines 25-45);

Authenticating the request (Column 9, lines 36-45; and Column 10, lines 26-40); and

Securely transmitting the access permission security profile from the server system to the network user over the network (Column 10, lines 41-49).

Regarding Claim 11,

Win as modified by Berson discloses the method of claim 7, in addition, Win discloses that the authorizing step is automatic and based upon the user's possession of an access permission security profile (Column 10, lines 26-40).

Regarding Claim 12,

Win as modified by Berson discloses the method of claim 7, in addition, Berson discloses that the encrypting step comprises:

Identifying a group of network users who are to be allowed access to a data object to be encrypted (Column 5, lines 20-35);

Generating an appropriate cryptographic credential key from a set of credential categories, the credential key relating to the group of network users (Column 5, lines 20-35);

Generating a cryptographic working key from at least a domain component (information for the state), a maintenance component (information regarding progression), and a pseudorandom component (Column 5, lines 20-35; Column 5, line 56 to Column 6, line 8; and Column 6, lines 55-65);

Encrypting the pseudorandom component with the credential key (Column 5, line 56 to Column 6, line 8; and Column 6, lines 55-65); and

Associating the encrypted pseudorandom component to the encrypted data object (Column 5, line 56 to Column 6, line 8; and Column 6, lines 55-65).

In this embodiment, the pseudorandom data is encrypted under the progressive credential keys, with a portion of the pseudorandom data being encrypted under each key.

Regarding Claim 13,

Win as modified by Berson discloses the method of claim 10, in addition, Win discloses that the access permission security profile is created by:

Identifying one or more groups of network users who are to be provided with cryptographic capabilities (Column 10, lines 26-49; and Column 13, lines 32-44); and

Creating one or more security profiles for each network user (Column 13, lines 32-44);

But does not disclose establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key, or that the security profiles contain at least one of these access codes.

Berson, however, discloses establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key (Column 3, lines 23-34; and Column 5, lines 20-35); and

That each network user's security profile contains at least one access code (Column 5, line 20 to Column 6, line 8).

Regarding Claim 14,

Win discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup or domain (Column 13, lines 32-44).

Regarding Claim 15,

Win as modified by Berson discloses the methods of claims 4 and 9, in addition, Win discloses that the request is initiated in-band by the network user over the network (Column 9, lines 25-35).

Regarding Claim 16,

Win as modified by Berson discloses the methods of claims 4, 9, 10, and 11; in addition, Win discloses that the access permission security profile is in the form of a token that is adaptable to expire (Column 10, lines 50-62).

Regarding Claim 18,

Win as modified by Berson discloses the methods of claims 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a hardware token (Column 27, lines 28-40).

Regarding Claim 19,

Win as modified by Berson discloses the methods of claims 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a software token (Column 17, lines 24-33).

Regarding Claim 20,

Win as modified by Berson discloses the methods of claims 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a user password (Column 9, lines 25-35).

Regarding Claim 21,

Win as modified by Berson discloses the methods of claims 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a record of time at which the request was made (Column 9, lines 46-52).

Regarding Claim 22,

Win as modified by Berson discloses the methods of claims 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a record of the user's physical location (Column 15, lines 46-60).

Regarding Claim 57,

Win as modified by Berson discloses the methods of claims 4 and 7, in addition, Win discloses that the decentralized public network is the Internet (Column 4, lines 46-57).

Regarding Claim 58,

Win discloses the method of claim 1 and the system of claim 52. Win as modified by Berson discloses the methods of claims 4 and 7.

Win discloses that the decentralized public network is a cellular phone network (Column 26, lines 32-47). Berson also discloses that the decentralized public network is a cellular phone network (Column 2, lines 9-21).

Regarding Claims 1 and 52, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the transition state-based cryptography system of Berson into the role-

based access control system of Win in order to allow an entire file, program, etc. to be downloaded/acquired at first, while controlling access to different/progressive sections of the data based upon predetermined conditions that the user must meet prior to decryption of the additional sections.

3. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Win in view of Woodward (Woodward, John, "Comments on Private Sector Use of Biometrics and the Need for Limited Government Action", 7/17/1998, pp. 1-12, obtained from http://www.ntia.doc.gov/ntiahome/privacy/mail/disk/Woodward.htm).

Win does not disclose that the authenticating step includes the use of biometric information.

Woodward, however, discloses that the authenticating step includes the use of biometric information (Pages 5-7, Section III). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the biometric searching techniques of Woodward into the role-based access control system of Win in order to provide a way to authenticate a user that is not based on a credential (such as a password) that can be easily compromised, thus enhancing reliability of the system's authentication.

4. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Win in view of Berson, further in view of Woodward.

Win as modified by Berson does not disclose that the authenticating step includes the use of biometric information.

Woodward, however, discloses that the authenticating step includes the use of biometric information (Pages 5-7, Section III). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the biometric searching techniques of Woodward into the role-based access control system of Win as modified by Berson in order to provide a way to authenticate a user that is not based on a credential (such as a password) that can be easily compromised, thus enhancing reliability of the system's authentication.

5. Claim 53 is rejected under 35 U.S.C. 103(a) as being unpatentable over Win in view of Shintani (U.S. Patent 6,137,480).

Win does not disclose that each client system further includes user authentication means.

Shintani, however, discloses that each client system further includes user authentication means (Column 2, line 61 to Column 3, line 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication card system of Shintani into the role-based access control system of Win in order to enhance service to a user and security of data on a computer by only allowing a user to use the computer when he is

authenticated and in close proximity to the computer, and by disabling access to the computer when the user leaves the computer.

6. Claim 53 is rejected under 35 U.S.C. 103(a) as being unpatentable over Win in view of Berson, further in view of Shintani.

Win as modified by Berson does not disclose that each client system further includes user authentication means.

Shintani, however, discloses that each client system further includes user authentication means (Column 2, line 61 to Column 3, line 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication card system of Shintani into the role-based access control system of Win as modified by Berson in order to enhance service to a user and security of data on a computer by only allowing a user to use the computer when he is authenticated and in close proximity to the computer, and by disabling access to the computer when the user leaves the computer.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffrey D Popham
Examiner
Art Unit 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER